A SURVEY on DENIAL-of-SERVICE ATTACK DETECTION METHODS

Suketha[1], Pooja N S[2]

[1]Department of CSE, SCEM, Karnataka, India
[2]Department of CSE, SCEM, Karnataka, India

ABSTRACT

Denial-of-Service (DoS) attack causes major impact on end systems by consuming their bandwidth and resources. DoS attack traffic behavior is completely different from the legitimate network traffic behavior so this paper presents a survey on DoS attack detection system using various methods. Later allowing only the normal traffic to enter the network and blocking the illegitimate traffic. It becomes necessary for developers and researchers to understand behaviour of the DoS attack because it affects the target network without any advance warning. DOS attacks typically aim services that are hosted on high-profile web servers such as card payment gateways and domain name servers.

Keyword : - *Denial-of-Service, Legitimate Network Traffic.*

1. INTRODUCTION

Denial-of-Service attacks are serious threat for interconnected systems. This attack can consume CPU, network resources, memory and also damages the operation of the resource which is under attack. These attacks prevent authorized users from consuming bandwidth and server resources. The victim can be a host, a router or an entire network. The major effect of these attacks varies from temporarily blocking service availability to misrepresenting the information in the network permanently.

DoS attack types: DoS attack can be categorized as

i. Ping of Death: This is caused by an attacker who is continuously sending ping packets that is larger than 65535 bytes. Many computer systems cannot handle such packets and also some systems get crash because of such a packets, this packet also result in buffer overflow.

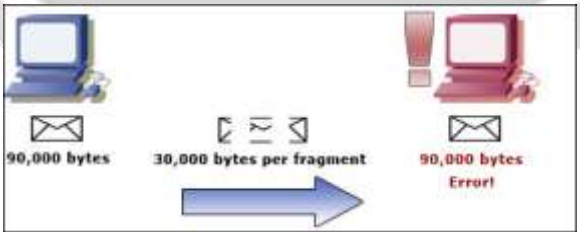

Fig. 1 Ping of Death attack

ii. Ping of Flood: This is caused by an attacker who is sending a huge mass of ICMP echo request(ping) packets. The floods of ping packets can consume significant bandwidth of the network.

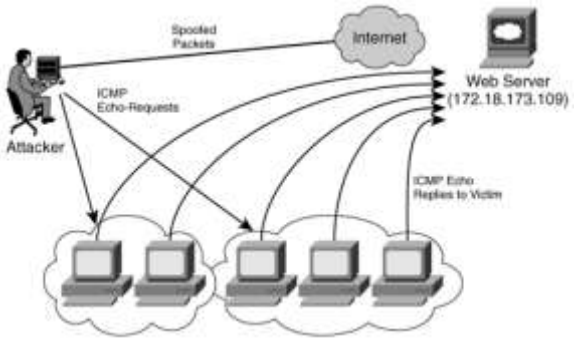

Fig. 2 Ping of Flood attack

iii. Smurf Attack: In this attack victim is flooded with ICMP packets. The packets more commonly uses the spoofed IP address in order to perform the attack result in lots of ping reply packets to the forged IP address.

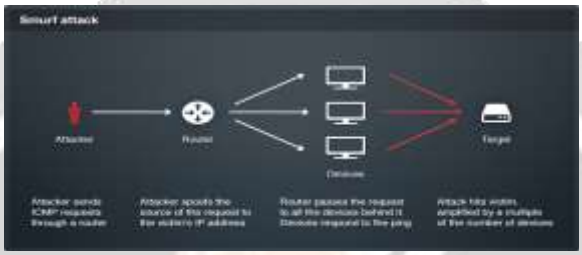

Fig. 3 Smurf attack

iv. Buffer overflow Attacks: Here attacker simply sends more traffic to the particular address with the aim of filling the buffer of that particular address. Sending ICMP packets larger than particular size, Sending mail attachments more than the particular limit are the some of the characteristics of buffer overflow attack.

v. Mail Bomb Attack: Receiving the large number of mail messages with large attachments from unauthorized users so giving a situation of Denial of Service to the authorized users.

.

2. LITERATURE SURVEY

2.1. Flow Correlation Coefficient Analysis Method

This is the method to detect DDoS attacks from crowds of network traffics[1].The approach achieves this by analysing the flow correlation factor among various flows. To analyse correlations the principal component analysis(PCA) technique is used here.Here botnets are engines.The detectors are made disable by botmasters by the reduction of traffic patterns of flash crowds.The method has a ability to detect the anomaly flows.

- **Advantages**: PCA finds the correlations among the features in a high dimension data by reducing the dimension of the data without losing the information in it.
- **Disadvantages**:It fails to produce better detection output in the form of better detection result and lesser false alarm result.

2.2. Covariance Matrix Based Method

This method was proposed in [2] for extracting the features correlation in the form of sequential samples.Main idea behind this technique is that some systems can be well described by the analysis of correlations among features of that system.The obtained correlation must be such that it should flag some changes between the features.Hence correlation acts as indicator to differentiate among normal traffic and abnormal traffic.

- **Advantages**: The advantage of this approach is it improves detection accuracy.
- **Disadvantages**: This approach is exposed to attacks because it continuously advances all the supervised features.

It considers group of features rather than individual feature and labels the whole group as either legitimate or illegitimate instead of individual feature of the group.

2.3.Triangle Area Based Method

This approach was presented in [3] to generate good quality selective features.

- **Advantages**:Generates high resolution selective features.
- **Disadvantages**: This approach addicted on advance knowledge of malicious activity. That means it will compare the observed traffic features with already known malicious activity.If there is no prior knowledge about the observed illegitimate traffic then this approach is of no use to analyse the attacks and also it not accurately detects the attack.

2.4. Geometrical Structure Based Method

Geometrical structure based approach is proposed in [4] here Mahalanobis Distance(MD) was used as threshold to obtain the correlations of selected packet payload for attack detection.

- **Advantages**:This approach not require advance information about malicious behaviours.
- **Disadvantages**:The main problem with approach is dependent on network packet payloads.

2.5.Sequential Change Point Detection Method

Sequential change point detection based DoS attack approach is presented in [5].This approach focuses on sequential data change of the observed traffic. The features may be management information base variables and characteristics between the number of SYN packets and the number of FIN or SYN/ACK packets.This method is applicable in areas such as industrial quality control, fault detection,finance,security systems ,clinical trials etc.

- **Advantages**: Effectively detects any dramatic changes in the network traffic.
- **Disadvantages**: The approach requires frequently updating of the operator matrix to cover the upcoming attacks and also suffers from time granularity problem. Ignores the correlative information which is important for accurate detection.

2.6.Change-Point Monitoring Method

The theory of CPM(Change Point Monitoring)[6] is based on the inherent network protocol behaviours. To make the detection mechanism insensitive to sites and traffic patterns, a non parametric Cumulative Sum (CUSUM) method is used.

- **Advantages**: CPM does not require per-flow state information and only introduces a few variables to record the protocol behaviours.The statelessness and low computation overhead of CPM make itself immune to any flooding attacks.
- **Disadvantages**: CPM has less detection latency and more accuracy.

2.7.Covariance Matrix Sign Method

An approach called Covariance Matrix Sign (CMS) for detection of DoS attack is proposed in [7].

- **Advantages**: The approach accomplishes high detection rates.
- **Disadvantages**: Suffers from problem of high false positive rates. This approach do not work properly in case of an attack changing all the previously monitored features.

2.8. Rank Correlation Based Detection Method

The number of packets in one flow has relationship with other flows based on this observation the method is proposed in[8].All packets to victim system at one particular router is considered as one flow. Let the two flows be 'F' and 'f' and it is considered as legitimate only if its correlation coefficient is close to one. In RCD(Rank Correlation Detection), as soon as an attack alarm raised, upstream routers obtains the rank relationship of malicious flows and uses this for further classification.

- **Advantages:** RCD is self reliant on protocol .Throughput is not altered by the cost of computation. Distinguishes attacking flow from the legitimate flow.
- **Disadvantages:** Performs rank correlation only for the ows which raises alarm.

2.9. Group Testing Based Approach

This approach[9] is represented by a binary matrix as t*n where ‘t’ represents pools and ‘n’ represents items.Detection process treats ‘t’ as virtual servers and ‘n’ as clients.Out of ‘n’ clients ‘d’ clients are assumed as attackers.The application is exactly deployed at the back end servers.This method will also detect the attacks at the

protocol layer.Negative pools are declared as negative there is no further tests.while the positive pools require further testing for proper detection of DoS attack.Clients are mapped into the columns of the matrix and servers are mapped into the rows of the matrix.Malicious activities are identified by the lack of resources at the server side. Virtual servers require enough resources to handle client requests.Back end servers acts as testing domains and virtual servers acts as testing pools.

- **Advantages:** Low detection latency. Low false positive/negative rate.
- **Disadvantages:** Managing the state of the virtual servers creates lots of overhead.

2.10. Emergent Self Organizing Maps

This approach [10] detects DoS attacks by comparing the normal traffic against the abnormal traffic.Emergent Self Organizing Maps can be applicable on areas including medical diagnosis and environmental science.Structure produced by Emergent Self Organizing Maps are visualized as distance based(U Matrix),density based(P Matrix),distance and density based(U* Matrix) and topology visualizations. The distance between successive points in the matrix represents the inconsistency of network traffic logs.

- **Advantages**: Very powerful method to detect DoS attack. High level structure is obtained by Emergent Self Organizing Maps.
- **Disadvantages**: High computational overhead.

2.11. Conditional Random Fields(CRF)

This method[11] employs signature based and anomaly based detection approaches. The method gathers traffic features such as source IP , destination IP ,source port entropy,destination port entropy etc. The approach collects all the entropies and fingerprints into a single vector to reflect the state of current traffic.This method needs to check the IP header value of each packets hence makes real time development easier .This method combines all the features into a single vector.Let X and Y represents two random variables , P(Y/X) represents the conditional probability distribution.This method contains various modules like data preprocessing to extracts the IP packet features, potential function definition, model training ,attack detection module to judge the monitoring traffic for DoS attack and output label etc.

- **Advantages**:It has a ability to detect upcoming DDoS attacks. High sensitivity and detection accuracy. Lower false positive alarms. It is independent of any type of DoS attacks.
- **Disadvantages**:Efficient under huge background network traffic.

2.12. Low Rate TCP DoS Attack Detection at Edge Routers

Low rate TCP DoS attacks[12] are different from the flood based attacks hence technique to detect such a attacks are necessary.Here flow is considered as malicious if its brust length is greater than or equal to Round Trip Times(RTT) of other flows of same server and time period must be same as minimum RTO.

- **Advantages**:Easily deployable.
- **Disadvantages**:Only applicable to low rate DoS attacks.

2.13. Random Early Detection Approach

This approach[13] is based on the flow trust value. Router is mainly used to monitor the network flows then it will calculates flow trust value for that corresponding ow.This flow trust value is used at queue management.Legitimate traffics are the ones which is having higher flow trust value.Malicious flow is the one which is having lower flow trust value.Trust value is used to evaluate the trustworthiness of the network entities.As soon as router receives packet, it forwards it to the network flow detection module where it is subjected to measure the flow size and packet loss ratio.Then it is forwarded to the trust evaluation module where flow trust value is computed.

- **Advantages**: Improves throughput and delay compared to other queue management approaches to detect DoS attack. Highly scalable.
- **Disadvantages**: Detects only flooding DoS attacks but fails to detect spoofing attack.

2.14.Channel Aware Approach

This approach [14] is used to find DoS attacks in wireless mesh networks.Victim router forwards a subset of packets but throws other packets.Channel aware approach efficiently identifies such a routers in a channel.This method is based on two policies such as channel estimation and traffic monitoring.If the packet loss at channel exceeds the normal loss rate then that particular node is declared as attacker.Each intermediate node along the given path implements downstream traffic monitoring.It will identifies intentional selective packet drops at particular channel.Each node maintains a packet count in order to measure the node loss rate.

- **Advantages**:Each node behaviour is monitored by upstream and downstream routers. To maintain detection accuracy with normal loss rate by adjusting threshold can be done. Detects the attacks and hence increases packet delivery ratio.
- **Disadvantages**:Not applicable in case of multiple malicious nodes.

3. CONCLUSIONS

DoS attack causes severe problems to authorized users by blocking the services.There are several methods to detect the DoS attack. Each method is suitable for detecting particular type of DoS attack. Hence some of the methods discussed above will be helpful for the detection of known and unknown DoS attacks and it will help to analyse the attack strategies and to find security solutions.

6. REFERENCES

[1] S. Yu, W. Zhou,W. Jia, S. Guo, Y. Xiang, and F. Tang,"Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," IEEE Trans. Parallel and Distributed Systems,vol. 23, June 2012.

[2] S. Jin, D.S. Yeung, and X. Wang,"Network Intrusion Detection in Covariance Feature Space," Pattern Recognition, vol. 40, 2007.

[3] C.F. Tsai and C.Y. Lin, "A Triangle Area Based Nearest Neighbors Approach to Intrusion Detection," Pattern Recognition, vol. 43,2010.

[4] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R.P. Liu, "RePIDS: A Multi Tier Real-Time Payload-Based Intrusion Detection System," Computer Networks, vol. 57, 2013.

[5] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E.Vzquez,"Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges," Computers and Security, vol. 28, 2009.

[6] Haining Wang, Danlu Zhang, and Kang G. Shin, "Change Point Monitoring Method to detect DoS attack",IEEE Transactions on Dependable and Secure Computing, vol. 1, October-December 2004.

[7] Tavallaee, S.A., Ghorbani, "A Novel Covariance Matrix Based Approach for Detecting Network Anomalies", IEEE, 2008.

[8] Wei Wei, Feng Chen, Yingjie Xia, and Guang Jin," A Rank Correlation Based Detection against Distributed Reflection DoS Attacks" IEEE Communications Letters, vol. 17, January 2013.

[9] Ying Xuan, Incheol Shin, My T. Thai, Taieb Znati," Detecting Application Denial-of-Service Attacks: A Group-Testing-Based Approach", IEEE Transactions on Parallel and Distributed Systems, vol. 21, August 2010.

[10] Aikaterini Mitrokotsa, Christos Douligeris, " Detecting Denial of Service Attacks Using Emergent Self-Organizing Maps", IEEE International Symposium on Signal Processing and Information Technology,2005.

[11] Shi-wen CHEN, Jiang-xing WU, Xiao-long YE, Tong GUO," Distributed Denial of Service Attacks Detection Method Based on Conditional Random Fields", Journal of Networks, vol. 8, April 2013.

[12] Amey Shevtekar, Karunakar Anantharam, Nirwan Ansari," Low Rate TCP Denial-of-Service Attack Detection at Edge Routers", IEEE Communications Letters, vol. 9, April 2005.

[13] Xianliang Jiang, Jiangang Yang, Guang Jin, and Wei Wei, "RED-FT: A Scalable Random Early Detection Scheme with Flow Trust against DoS Attacks",IEEE Communications Letter, vol. 17, May 2013.

[14] Devu Manikantan Shila,Yu Cheng,Tricha Anjali,"Mitigating Selective Forwarding Attacks with a Channel-Aware Approach in WMNs", IEEE Transactions on Wireless Communications, vol. 9, May 2010.